ARAT Bulletin

Electronic Combat

January 1999
Volume 4, Issue 4

"Serving the Army Reprogramming Community Since 1994"

Inside this Issue

1 ARAT-TA Update

2 From the Project Officer's Desk

2 MLV Update

3 MSEWBBS—Update

4 Special Feature—Should I Use MSEWBBS/WEB or SIPRNET?

5 Flagging Update

6 Springtime in Paris—A Report on the AOC Conference

7 FiestaCrow '99

12 For Your Information
- Coming Events
- Points of Contact

The Quarterly Professional Bulletin Published by the Army Reprogramming Analysis Team—Project Office (CECOM Software Engineering Center)

ARAT-TA Update

Busy, Busy, Busy as Usual

By The ARAT-TA Team

Although the *ARAT Bulletin* has been on vacation for some time, the Army Reprogramming Analysis Team-Threat Analysis (ARAT-TA) has not enjoyed the same luxury. Worldwide threat analysis, Mission Data Set (MDS) development and distribution, and Signal Flagging operations continue to occupy center stage for the 13 members of the Threat Analysis Team.

Keeping Busy with Major Tasks

Most activity has focused on support for the AN/APR-39A(V) family of Radar Signal Detecting Sets (RSDS). During 1998, ARAT-TA has:

- Completed detailed threat analyses to support development of 16 separate regionalized MDSs. [-39A(V)1]

- Fielded seven data sets for aviator use—five were block cycle updates and two were new. [-39A(V)1]

- Completed five data sets that are ready for final simulation testing at CECOM SEC; four others are being finalized at ARAT-TA. [-39A(V)1]

In addition, we have supported a significant number of threat analyses and mission data set developments for the -39(V)2, -39A(V)3, and the Navy/USMC's new -39A(V)2.

Of course, MDS production also involves development, integration, and use of flagging models for each MDS. The three members of the Threat Analysis Team at the Air Force Information Warfare Center, Kelly AFB, TX, build and maintain these flagging models. APR-39 users might think of the flagging models as early warning devices; these sophisticated software tools alert ARAT-TA engineers to changes in signals of interest. Based on subsequent analysis, MDS changes might be warranted. [For more information on this key element in the reprogramming process, read the article on page 5 written by Carl Brunner, one of our resident "flag wizards."]

ARAT-TA's production capabilities have significantly improved since the first data set we prepared in 1994/95. That MDS took almost seven months to complete, from initial threat analysis to fielding. Concurrently with improvements in throughput, our hardware and software tools have been continuously upgraded. Based on lab simulations and flight testing, we have also gained important insights into the operation of the AN/APR-39A(V) systems. The cumulative results of these advances provide more efficient processes and higher-quality products, but the most important benefit is increased survivability for all users of the AN/APR-39A(V) family.

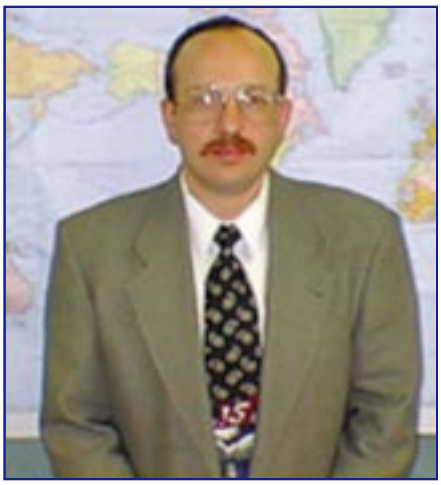
See "ARAT-TA Update" on page 7

From the Project Officer's Desk

Teamwork and Interdependence

By Joe Ingrao, ARAT Project Officer

As within many organizations, warfighters must mutually rely upon each other for both their safety and mission success. Teamwork and interdependence are easy to talk about, difficult to enculturate, and can never be completely ensured. During this last year, we have received numerous calls and e-mails from field users requesting Rapid Reprogramming instructions and information. Many of the inquiries came from newly assigned Electronic Warfare Officers (EWOs) wanting to establish ARAT communication accounts or requesting software reprogramming kits. Since our military personnel's assignments are constantly in a state of flux, it is imperative for the ARAT team to orient the EWOs and reprogramming personnel as quickly as possible. It is our charter and responsibility to develop a seamless and proactive reprogramming environment to ensure Warfighter safety and mission success. We welcome the inquiries from the *U.S. Army EWOs*—our Rapid Reprogramming teammates.



It's Good To Be Back!!

MLV Update

Windows95™ Version of MLV Kit Coming

By Jon Cory, SRI International

Memory Loader/Verifier (MLV) reprogramming kits for the AN/APR-39A(V)1 are now available worldwide through a logistics tracking and distribution plan developed and managed by the Army Reprogramming Analysis Team Project Office (ARAT-PO) in coordination with CECOM LARs. More than 150 MLV kits have already been distributed to users, and additional MLV kits can be ordered through any CECOM LARs or by contacting ARAT-PO directly.

The original MLV software, completed in 1995, was developed using C++ with DOS 5.0. SRI recently completed a Windows95™ upgrade version of the MLV software, and the ARAT-PO is in the process of distributing copies to all of the DOS-based MLV kit users. All future distribution of MLV kits will have both the DOS-based version and the Windows95™ upgrade version. There is a conflict within the communications library of the DOS-based version when employed with newer PCs, so the Windows95™ version should be used with any machine that is capable of running Windows95™. If you have an MLV kit and have not received the Windows95™ upgrade version, please contact ARAT-PO.

The Multi-Service Electronic Warfare Bulletin Board System (MSEWBBS)

By Roy Williams and Jim Harrison, SRI International

The concept and operation of the MSEWBBS (hereafter referred to as BBS) remains unchanged since the last *ARAT Bulletin* was published nearly a year ago. However, that doesn't mean that the system itself is static. Quite the contrary! For users accessing the BBS via Secure Internet Protocol Router Network (SIPRNET), the BBS Web Page is now browser-capable. In the past year, new server hardware, an upgraded operating system, and upgraded application software have been incorporated. For system power backup, emergency generators have been permanently installed, and an off-site mirror system capability has been successfully demonstrated. In fact, in anticipation of a hurricane that recently threatened Eglin AFB, the System Operators (SYSOPS) were ready to relocate all operations to an inland site to ensure continuous Warfighter support. Behind the scenes, continuous software and hardware evaluation, testing, and integration are being accomplished. This upgrade process is completely seamless to the user community, yet is an essential prerequisite for providing strong support to the Warfighter.

RELIABILITY—The system has proven extremely reliable. It operates 24 hours a day, 365 days a year. In fact, since its inception, the BBS has been available to users more than 97% of the time. The remaining 3% includes the brief "downtime" for daily scheduled maintenance. If you have attempted to log on to the system, but were unable to complete the connection, the SYSOPS were probably performing that daily maintenance—a process that requires about 30 minutes. Since this is usually done from approximately 1315-1345 Zulu, you might plan to avoid calling during that period.

ACCESS—The BBS server does not care how you contact it, whether via Secure Telephone Unit (STU), SIPRNET, Multiple Subscriber Equipment (MSE), or other electronic means. But, you cannot gain access without a personal account. Getting aboard the BBS is simpler than ever. Complete details on how to establish an account are available from the Army Reprogramming Analysis Team– Threat Analysis (ARAT-TA) [see related article in this issue]. An updated User Guide, published in draft format in June 1998, contains everything you need to know about access requirements and application procedures. It also contains illustrated directions on software and hardware configuration and setup, as well as an expanded section on troubleshooting. If you do not currently have a BBS account, call or email us; information will be sent to you immediately.

USERS—The BBS will currently support simultaneous access of 48 users via STU dialup and 72 users via SIPRNET. As of 1 Nov 98, more than 1700 accounts were active from 335 units from all services. This figure represents approximately 260 USAF units and more than 20 Navy/Marine sites (sites such as aircraft carriers usually have multiple units on the BBS). Surprisingly, even though the U.S. Army has more Aircraft Survivability Equipment (ASE) fielded than all other services combined, only about 55 units have BBS accounts. Considering that the BBS is the only source for Mission Data Set (MDS) updates for the AN/APR-39A(V)1 Radar Signal Detecting Set, what's wrong with this picture?

Y2K—Will there be any problems with the infamous "Year 2000" issue? As far as the BBS SYSOPS are concerned, no. All existing software and hardware have been tested and verified as Y2K-compliant, and the staff is aggressively monitoring future system upgrades to ensure a seamless transition into the next century.

HOT TIP—You say that you don't have a dedicated computer for classified BBS access or reprogramming, and the Commanding Officer won't cough up the bucks to purchase one? If you or an associate have regular Internet access, get on the Internet and point your browser to:

http://www.disa.mil/cio/darmp/excess.html#excess%20files

The Government recycles small computers, and the Defense Information Systems Agency acts as a nationwide clearinghouse. This is an excellent source to obtain one or more FREE computers and other computer equipment. Check it out!

A WORD TO THE WISE—Finally, for you "occasional" BBS users (and you know who you are)—that old saying about "absence making the heart grow fonder" does not apply to BBS accounts. To put it another way, the server is programmed to automatically purge accounts from the system if they haven't been accessed in a specified period of time. So, if you attempt to log on and discover that your account no longer exists, you will have to contact the BBS SYSOPS to reestablish access. Should you urgently be needing different or updated ASE MDS files, this would be a most untimely setback. Therefore, we hope to see you logged aboard the BBS on a regular basis.

Should I Use MSEWBBS/WEB or SIPRNET? And Why? You have questions? We have answers!

By Andrew Lombardo, Ilex Systems

When supporting unit ASE/EWOs, the ARAT-PO continues to encounter confusion over what an "ARAT" account is and what capabilities/data access it can provide to the user. This article, presented in the form of questions about user requirements, clarifies the differences and capabilities between an MSEWBBS/WEB account and an ARAT dial-up SIPRNET account. By answering the following questions, you will be able to more clearly state your requirements, and thus, we will be better able to rapidly meet your needs.

1. Do you require access to the Mission Data Set (MDS), Tactics, Techniques, and Procedures (TTP), and other related threat data files for reprogrammable systems like the AN/APR-39A(V)1?

If so, then you need an account on the Multi-Service Electronic Warfare Bulletin Board System (MSEWBBS). This is a data server located at Eglin AFB, FL, that is a repository for the MDS and other files that you are interested in gaining access to. An MSEWBBS account will also enable you to exchange email with other MSEWBBS account holders.

The Army POC for this system is Mr. Robert Hankins. However, any of the Air Force administrators at Eglin AFB can also help you. Their phone# is DSN (312) 872-2166, CML (850) 882-2166, and their Internet email address is: msecbbs@eglin.af.mil. (Note: Use of DSN area codes may be optional for your calling area.)

To attain an MSEWBBS account, you need to fill out a memo following the example enclosed in the February 1997 *ARAT Bulletin*. Have your Terminal Area Security Officer (TASO) send it to the Eglin MSEWBBS admin staff, together with your clearance information from your S-2. If you do not have the example memo, contact the MSEWBBS staff, download it from the Internet/NIPRNET ARAT website at URL:

http://arat.iew.sed.monmouth.army.mil/ARAT/forms/forms.htm
-or-
http://192.25.151.17/ARAT/forms/forms.htm
(if you don't have Domain Name Service (DNS) available at your site)

or contact the ARAT-PO who can email/fax/mail it to you (the ARAT-PO POC is Ms. Fanny Leung; her contact information is detailed below in question #3).

To gain dial-up access to the MSEWBBS, you will need the following hardware/software (HW/SW) at a minimum:

a. Secure Telephone Unit (STU-III)/Secure Terminal Equipment (STE).
b. An accredited computer (CS3 level–collateral SECRET) with an available communications (COM) port.
c. A terminal emulation SW program like Procomm Plus for Windows/DOS, or HyperTerminal (comes bundled with Microsoft Windows95/98).

The phone numbers for Army users to dial into the MSEWBBS via STU-III/STE are:

Toll Free (CONUS only) 1-800-895-0604, CML (850) 883-1806, DSN (312) 875-1806

The terminal emulation SW, your Operating System (OS) SW, and your STU-III/STE will have to be properly configured to be able to dial-up and connect to the MSEWBBS successfully. Configuration assistance is available from the MSEWBBS admin staff. A step-by-step configuration guide for HyperTerminal can be found in the September 1997 *ARAT Bulletin*. Past issues of the *ARAT Bulletin* can be accessed from the ARAT Internet/NIPRNET website at URL:

http://arat.iew.sed.monmouth.army.mil/ARAT/bulletin/bulletin.htm
-or-
http://192.25.151.17/ARAT/bulletin/bulletin.htm
(if you don't have DNS available at your site)

See "Questions & Answers" on page 8

Shop's Capabilities Continue to Improve

By Carl Brunner, SRI International

Since its establishment in 1995, the ARAT-TA flagging shop has continued to develop its capabilities to support rapid reprogramming. The flagging shop—the front end of the reprogramming process—is located in San Antonio, TX, and shares space with the Air Force Information Warfare Center (AFIWC), where the Air Force performs its flagging function. The three people who staff the shop glean from the thousands of signals collected each day the few that Army Target Sensing Systems (ATSS) cannot identify. The flagging shop is quite small, given the magnitude and significance of its task. But since the last update discussed in the *ARAT Bulletin*, the flagging shop has improved its manning and its data accessibility, and is adding new flagging models to inventory.

ARAT-TA Assigns ELINT Analyst

Three types of personnel skills are needed to complete flagging tasks:

- The flagging engineer, who has detailed knowledge of the ATSS and designs the flagging model.
- The computer scientist, who codes the models and maintains a variety of data and knowledge bases to automate the flagging process.
- The ELINT analyst, who performs quality control of incoming signals and manually identifies emitters that the expert systems cannot.

In the past, ARAT-TA had depended on the Air Force to provide ELINT support. However, in late 1997, ARAT-TA assigned an active duty soldier, SSG Edward L. Wiggins, to the flagging shop to fill the ELINT analyst slot. With the arrival of SSG Wiggins, ARAT-TA has all the requisite skills to run the flagging shop independently. SSG Wiggins is the only government employee in the flagging shop, so he represents the Army in its dealings with the AFIWC and the Air Intelligence Agency. He has been an outstanding addition to the flagging shop.

However, all positions are manned only one deep. SSG Wiggins is working on a partial remedy by asking the 748 MI BN to augment the shop's staff with their ELINT analysts for contingencies and exercises. Initial response has been positive, and SSG Wiggins plans to train the augmentees periodically on flagging operations. So, although the flagging shop's manning is minimal, ARAT-TA has all the necessary skills and is developing the ability to assume continuous operations.

Faster Access to Databases

The ability to operate continuously now includes the ability to access flagging data anytime and anyplace with SIPRNET connectivity. The Conventional Flagging Data Base (CFDB) is a relational database that (1) contains all signals outside the limits of the mission data sets of the various ATSS, and (2) links the response of the ATSS flagging models to the signals. The CFDB contains more than 2800 flags for Army mission data sets. The CFDB is available on a server connected to SIPRNET, and ATSS system analysts and engineers can query the database using a graphical user interface (GUI) designed specifically for CFDB. The GUI allows the data to be accessed and sorted in a variety of ways according to the user's particular requirements.

The CFDB and GUI compose the Flagging Data Management System (FDMS), which has been on line for a year. ARAT analysts, who have used FDMS to develop new mission data sets in theaters throughout the world, have been pleased overall with the system's performance but have expressed a desire to increase data retrieval speed. The nature of the SIPRNET network can delay data retrieval by several minutes as the request works through the various nodes. To improve the retrieval speed, ARAT will install a copy of the database at the Eglin AFB site and update the database remotely. The ultimate goal (contingent on the availability of funds) is to have the Eglin server mirror the server at the AFIWC, which will require a software upgrade. The improvement will speed flagging analysis and will increase user acceptance of the CFDB.

Working on RSDS Models

While development on the FDMS continues, additional flagging models are under development to broaden ARAT support of ATSS. The hardware and software for the AN/APR-39(V)2 Radar Signal Detection Set (RSDS) have been upgraded, thereby allowing it to be reprogrammed in the field and supported by ARAT-TA. In response, the flagging shop has developed a flagging model for the RSDS that is currently in the debugging phase. Soon, this model will be implemented and will provide flagging support for the series of new mission data sets being developed for the RSDS. Following completion of this model, development will begin on another flagging model: the AN/APR-39A(V)2—a brand new RSDS that will be used by the Marines. ARAT-TA will provide flagging and mission data reprogramming support for the system. This is the first joint venture between the Army and the Sea Services in rapid reprogramming. The success of this venture could lead to greater interservice cooperation in this area.

Shop Capabilities Improving

The ARAT-TA flagging shop has continued to improve in a period of lean budgets and staffing. Capabilities are improving in its ability to operate continuously, to provide data access, and to support more ATSS. The flagging shop envisions new ways to improve the quality of its service and data and continues to monitor technological innovations that could contribute to the flagging process. Although the flagging shop is the lead element in the reprogramming process and far from the field, it is always mindful that its job is to support the soldier.

Springtime in Pa-ree!

By Pete McGrew, SRI International

Dateline: PARIS—The Eiffel Tower, the Louvre, the Arc de Triomphe, and the River Seine were the classic backgrounds to the very successful May 1998 Association of Old Crows (AOC) International Conference and Exposition. The Exposition, which was held in a large convention area within the Louvre Museum, drew superb attendance. The opportunity to enjoy gourmet delights of French cuisine and wine—and then to discuss and display modern capabilities surrounded by some of the world's most treasured works of art—doesn't happen too often.

At the show, the Communications Electronics Command Software Engineering Center, Electronic Combat (CECOM SEC EC) fielded a demonstration booth to "advertise" its capabilities and successes in bringing reprogramming to Army Target Sensing Systems (ATSS)—specifically, lightweight Aircraft Survivability Equipment (ASE). The purpose of this reach-out effort by CECOM SEC EC was to reinforce to NATO and our other allies (who use identical or modified Army-lead ASE) that the communication methodologies and optimization of data programmed into ATSS is a dynamic and important program. Monitoring the potential areas of direct combat, peacekeeping operations and non-combat evacuation scenarios puts all our users at risk if we do not have the infrastructure to rapidly and confidently update those systems.

The CECOM SEC EC booth featured a large backdrop display emphasizing the CECOM SEC structure and the programs it manages throughout the world. One of the two side tables was configured with an AN/APR-39A(V)1 Radar Signal Detecting Set (RSDS)—the world's mostly widely fielded reprogrammable, lightweight radar warning system. This display included a test stand and a laptop computer connected to the RSDS with the inexpensive but highly effective CECOM SEC EC reprogramming/upload cable. The other side table was configured with a monitor and a laptop computer that displayed a brief video explaining the reasons why rapid updating is a relevant requirement, how it is done for the U.S. Army RSDS, and the benefits of making those changes expeditiously.

Military and government attendees included those from as far away as Singapore and as close as the French Government offices adjacent to the Louvre. Companies and organizations exhibiting were from as far afield as California to Italy. The CECOM SEC EC personnel assigned to the Exposition, who had numerous discussions with a variety of people from diverse backgrounds, were able to demonstrate the reprogramming and RSDS uploading process. It was evident from comments received that ease-of-use and cost were important factors to these individuals. These discussions and demonstrations are important because they lay the groundwork for the support of U.S. ASE in Foreign Military Sales programs.

The Convention and Symposium lasted three days. During the Symposium portion, various companies and different government organizations delivered technical briefings on topics covering:

- Infrared and RF countermeasures
- Solid-state technologies
- Digital technologies for electronic support measures and countermeasures
- Receiver technologies
- New naval vessel construction, and
- Aircraft Electronic Warfare (EW) efforts.

For the first time in the AOC's history, the Russian Deputy—Mr. Alexi Shoulounov of the State Radio Technical Institute of Moscow—was allowed to brief his view of the EW world, specifically new trends in electronic countermeasures. After his speech, he answered some general questions posed by a CECOM SEC EC member. The Deputy was courteous but somewhat nebulous in his answers!

The AOC is an organization that espouses the understanding, use, and capabilities of EW. The CECOM SEC EC booth, displays, and qualified assigned personnel did much to support those qualities, and at the same time inform many people of CECOM's on-going ASE reprogramming efforts and capabilities.

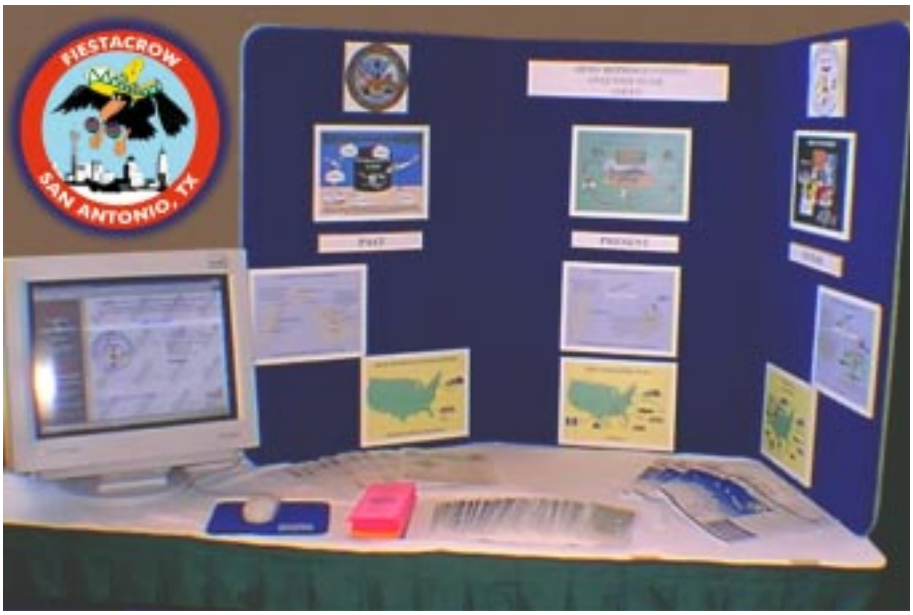
C'est la vie!

FiestaCrow '99

By Tara Hurden, SRI International

Ola! It's time again for FiestaCrow, the Association of Old Crows annual symposium held during Fiesta Week, 18-21 April 1999, in San Antonio, TX. This year's symposium centers around "Information Operations Going Global." The Army Reprogramming Analysis Team (ARAT) and CECOM Software Engineering Center (SEC) will be displaying its Rapid Reprogramming capabilities and support to the U.S. armed forces as well as to Foreign Military Sales (FMS) customers. We urge everyone to visit our booth and take advantage of the Electronic Warfare Rapid Reprogramming Demonstrations we will be exhibiting.

Further information on FiestaCrow'99 can be found at www.fiestacrow.org or by calling the Billy Mitchell Chapter Office at 210-732-7697. Look forward to seeing y'all there!



The ARAT Information Display at the AOC Guardrail Symposium (June 1997)

ARAT-TA Update

Continued from page 1

Other Tasks Occupy "Spare Time"

When we aren't "crunching numbers," numerous other tasks also demand our attention: the Multi-Service Electronic Warfare Bulletin Board (MSEWBBS), Aviator Training, and development of rapid reprogramming capabilities in emerging Army Target Sensing Systems (ATSS).

As you know from earlier *Bulletin* articles, the MSEWBBS secure communications system provides the backbone for distribution of all rapidly reprogrammable Army ATSS Mission Data Sets. One member of the ARAT-TA team at Eglin AFB provides full-time support as a System Operator (SYSOP) for the MSEWBBS. Hosted by the USAF's 53rd Wing, the Army portion of the MSEWBBS requires a concerted effort for account management, customer service, and system maintenance. Mr. Bob Hankins ably serves as ARAT-TA's representative on the MSEWBBS, and fields dozens of calls daily. As mentioned in a separate *Bulletin* article, users of the AN/APR-39A(V)1 require MSEWBBS access to obtain MDS updates; it's the only way to get them. If your organization isn't aboard, it's definitely in your best interest to give Bob a call.

The nearly world-famous ARAT "Away Team" continues to conduct aviator training on Aircraft Survivability Equipment (ASE). Schedules permitting, one or two of the engineers from our Eglin AFB site travel to Ft. Rucker, AL, on a monthly basis. The purpose of these trips is to acquaint students at the Aviation Center's Electronic Warfare Officer Course with Army reprogramming concepts, products, and support organizations. On a larger scale, team members periodically visit Aviation Brigades to conduct technical training on the operation and reprogramming of ASE. A recent training trip to U.S. Forces, Korea, was combined with an investigation of signal anomalies, and included numerous AN/APR-39A(V)1 flight tests on an instrumented Electronic Warfare range. We have also given brief presentations at two of four Army National Guard Aviation Classification and Repair Activity Depots. Regardless of the type, scope, or duration of these training visits, our goal is to increase awareness of the support capabilities and products available from the Army Reprogramming Analysis Team.

Continued on page 8

ARAT-TA Update

Continued from page 7

As directed in Army Regulation 525-15, new ATSS must incorporate provisions for "rapid" reprogramming. Therefore, the Threat Analysis Team has continued interaction and coordination with numerous program offices and defense contractors to support incorporation of reprogramming capabilities in ATSS systems under development or undergoing weapon system integration. Typical systems include the AN/APR-39A(V)2, AN/AVR-2A, SADARM, WAM, BAT, and the AN/ALQ-211 Suite of Integrated RF Countermeasures Set (SIRFC). Through continuous involvement in these programs, we can provide the benefits of "reprogramming lessons learned" to help field more efficient and more capable ATSS systems.

One of the ATSS subsystems currently fielded with the AH-64D LONGBOW Apache does not meet the requirements for "rapid" reprogramming and is now suffering the consequences. The LONGBOW Fire Control Radar system's AN/APR-48A Radio Frequency Interferometer (RFI) still requires the Unit Data Module (UDM) be removed from the set, placed on a lab bench, and reprogrammed via a PROM burner. This is a very costly, labor-intensive, and logistically challenging process.

Efforts are currently under way to reprogram the RFI worldwide Mission Data Set (MDS). This will be a two-phase effort:

- Update the existing worldwide MDS to support an impending redeployment.
- Develop a long-term MDS maintenance plan and rapid reprogramming capability to support future updates and geo-tailoring.

The tentative schedule for this reprogramming effort calls for completion of the analysis and coding process by the end of December 1998, completion of testing by the end of February 1999, and completion of the actual equipment reprogramming process by 15 March 1999. Unfortunately, availability of time and money will not allow all the signal parameters in the UDM to receive an update during this reprogramming effort. However, it should establish a baseline for future reprogramming efforts and will focus on updating the threat systems most likely to be encountered by the Longbow aviators in the region in which they will be deployed. The manufacturer will code, test, and electronically update the UDM in both the fielded and soon-to-be fielded RFI systems. ARAT-TA will provide threat analysis and quality control of the threat parametric data prior to the actual reprogramming of the UDM. Once the data have been gathered, verified, and coded, they will be tested in the laboratory at the LMFS facility. ARAT-TA personnel will monitor this testing to ensure the system responds properly to the programmed data with no degradation in system performance. ARAT-TA remains committed to long-term support of future AN/APR-48A RFI reprogramming efforts. We are hopeful that system modifications in the near future will bring the RFI reprogramming process more in line with AR 525-15 requirements and other ATSS.

Talk to Us

Although those of us supporting the Threat Analysis Team occasionally feel that "the only thing constant is change," most changes have resulted in better support to our customers: the Warfighters. As a parting shot, we ask that you provide us feedback. We value your input and want to hear from you in the user community, whether your comments are brickbats or bouquets. The Threat Analysis Team depends heavily on your feedback to ensure that changes under consideration benefit *you*.

Questions & Answers

Continued from page 4

2. You can also gain access to the MSEWBBS through the Multi-Service Electronic Warfare Web (MSEWWEB) via the Secure Internet Protocol Router Network (SIPRNET). It has the same look and feel as the Internet, except the data lines are encrypted at the SECRET Collateral level. Do you have SIPRNET access already at your unit?

If so, then you can use your web browser to connect to the MSEWWEB/MSEWBBS on SIPRNET. Just like on the Internet, the SIPRNET has a World Wide Web (WWW) known as INTELink-S, which provides access to intelligence reports and information from a vast number of National Intelligence Community agencies like the Defense Intelligence Agency (DIA), the National Ground Intelligence Center (NGIC), and the National Imagery and Mapping Agency (NIMA), to name just a few. The MSEWWEB/MSEWBBS can be accessed at the following SIPRNET URL: http://207.84.75.101/LOGON/log2.htm

Continued on page 9

On that web page, the "telnet" link will provide a "DOS-like" terminal emulation connection to the MSEWBBS where you can access your email account and other information. The "file downloads" link will display the available MSEWBBS libraries and files, and permit downloading of files via a web interface. Another option for PC users having SIPRNET access is Galacticomm's WorldGroup Manager SW, available for downloading from the MSEWBBS library "BBSOPS." The SW file is entitled "MSEWCLNT.exe" (2.36 MB); the installation procedures are documented in "WGINST.doc." The MSEWBBS admin staff can also provide assistance concerning the installation, configuration, and use of the WorldGroup Manager SW.

As indicated above, the MSEWWEB site is accessible via SIPRNET/INTELink-S and contains links to all the data files located on the MSEWBBS. The data files can be accessed/downloaded from the MSEWWEB, provided you have an MSEWBBS account (userid and password), obtained in the manner detailed in question #1 above.

3. If your unit does not have direct SIPRNET access, do you desire dial-up SIPRNET access?

The ARAT-PO can establish an ARAT account for you that will enable dial-up SIPRNET access via STU-III/STE (just like dialing an ISP from home). This ARAT account will provide you access to the INTELink-S WWW as well as a SIPRNET-wide email address that you can use to exchange email with anyone on SIPRNET. The ARAT-PO POC for attaining an ARAT account and gaining dial-up access to SIPRNET is Ms. Fanny Leung. Her phone# is DSN (312) 992-1859, CML (732) 532-1859, and her Internet email address is: leungf@mail1.monmouth.army.mil.

To get an ARAT dial-up SIPRNET account, you need to fill out an ARAT account form following the example in the February 1997 *ARAT Bulletin* (although it has been recently updated and is thus slightly different) and send it to Ms. Fanny Leung, together with your clearance information from your S-2 and your computer's accreditation paperwork from your TASO/IMO/AMO/ISSO personnel (depending on what your unit designates it as). If you don't have the latest ARAT account form, you can download it from the Internet/NIPRNET ARAT website at the URL given in question #1 above, or Ms. Fanny Leung can email/fax/mail it to you.

To gain dial-up access to SIPRNET, you will need to have the following HW/SW at a minimum:

a. STU-III/STE
b. An accredited computer (CS3 level – collateral SECRET)
c. TCP /IP /PPP (Transmission Control Protocol/ Internet Protocol / Point-to-Point Protocol) SW like Trumpet Winsock or the version that comes bundled with Microsoft Windows95/98
d. Web browser SW like Netscape or Microsoft Internet Explorer

Your browser, TCP/IP/PPP, and OS SW, as well as your STU-III/STE, will have to be properly configured to be able to dial-up and connect to SIPRNET successfully. A step-by-step configuration guide for Trumpet Winsock can be found in the December 1997 *ARAT Bulletin*. Past issues of the *ARAT Bulletin* can be accessed from the ARAT Internet/NIPRNET website at the URL given in question #1 above. Further configuration assistance is available from the ARAT-PO technical staff at DSN (312) 992-9395/9392, CML (732) 532-9395/9392 or by contacting Ms. Fanny Leung.

4. Are you located OCONUS and need dial-up SIPRNET access?

The Defense Information Systems Agency (DISA) has established dial-up communications servers (comm servers) in all theaters, CONUS and OCONUS. It is much easier to dial an in-theater telephone number than to dial a CONUS number from OCONUS (you usually need authorization from the unit/command, a control number from the operator, and the connection can be preempted). A DISA Comm Server account requires the same HW/SW items mentioned in question #3 above. If you are OCONUS and need SIPRNET dial-up access, contact the appropriate theater POC below who can assist you with what is required to attain this service.

Continued on page 10

Continued from page 9

- Pacific: Mr. Steve Barnes
  DSN (315) 438-8220, CML (808) 438-8220
  email: pachostr@shafter-emh3.army.mil
  (By the time this article is published, Steve has indicated that he will most likely have had a change of duties. Unfortunately, at the time that this is being written, a replacement has not been selected, but the email address should still be correct for the new representative)

- Europe: Ms. Brigitte Schork
  DSN (314) 380-4031
  email: brigs@giis.tnoc.5sigcmd.army.mil -or- brigs@hq.5sigcmd.army.mil
  (Brigitte has indicated that she can point the user to the correct POC based upon their unit)

- Overall Army POC: Ms. Linda Jones
  DSN (312) 879-6840, CML (520) 538-6840
  FAX (520) 533-6809
  email: domain-request@huachuca-giis.army.mil -or- jonesl@hqasc.army.mil

- Alternate Army POC: Mr. Gil Castro
  DSN (312) 879-6499, CML (520) 538-6499
  FAX (520) 533-6809
  email: gcastro@huachuca-giis.army.mil
  (Contact the Army representative if you are located in CONUS or cannot get the needed assistance from your theater representative)

The DISA comm server account form is available for download from the Internet/NIPRNET ARAT website at the URL given in question #1 above.

In summary,

A. If you require access to the MSEWBBS data files, fill out and submit the MSEWBBS account memo and security clearance information to Mr. Robert Hankins at Eglin AFB, FL. An MSEWBBS account (userid and password) is needed by those who are directly dialing into the MSEWBBS server itself via STU-III/STE, as well as those who are accessing the MSEWBBS through the MSEWWEB via a direct SIPRNET connection or a dial-up SIPRNET connection.

REPEAT: Regardless whether you access the MSEWWEB through a direct connection or a STU-III/STE dial-up SIPRNET connection, you will still need to apply for an MSEWBBS account to be able to log in and access the data files.

B. If you require an MSEWBBS account and dial-up SIPRNET access, and are in CONUS, contact Mr. Robert Hankins at Eglin AFB for the MSEWBBS account (see A. above). Also, complete an ARAT dial-up SIPRNET account form and forward it, along with your clearance and computer accreditation information, to Ms. Fanny Leung at Fort Monmouth, NJ.

C. If you require an MSEWBBS account and dial-up SIPRNET access, and are OCONUS, contact Mr. Robert Hankins at Eglin AFB for the MSEWBBS account (see A. above). Also, contact the appropriate theater POC (listed in question #4 above) to request a DISA Comm Server account. They will inform you about what they need based upon their theater's policies.

D. If you just require dial-up SIPRNET access, contact Ms. Fanny Leung (if you are in CONUS) or your theater DISA POC (if you are OCONUS).

E. All the necessary forms/memos and examples are available for downloading, in both text and zipped MS Word 6.0 formats, from the ARAT Internet/NIPRNET website at the URL mentioned in question #1 above.

Continued on page 11

Continued from page 10

Bottom Line—The MSEWBBS administrative staff at Eglin AFB, FL, handles the MSEWBBS accounts, whereas the dial-up SIPRNET access accounts for CONUS users are administered by the ARAT-PO staff at Fort Monmouth, NJ. OCONUS users desiring dial-up SIPRNET access accounts should contact their theater DISA representative for more details. The Fort Monmouth ARAT-PO staff can assist you in contacting and forwarding your MSEWBBS paperwork to the MSEWBBS admin staff at Eglin or your dial-up SIPRNET account application to the appropriate DISA representative, as well as provide configuration assistance for your HW/SW and STU-III/STE.

Before contacting the ARAT-PO staff, please determine your HW/SW capabilities and requirements by completing the self-survey below. The information will be useful to the ARAT-PO technical staff in helping you determine your requirements and in attaining what you need to achieve the proper access/connectivity.

MSEWBBS/SIPRNET Self-Survey

STU-III/STE Make _____ Model _____

STU-III/STE Secure Data Rate (bps): ☐ 14400 ☐ 9600 ☐ 4800 ☐ 2400

Does your STU-III/STE have remote control capability? ☐ Yes ☐ No

Hardware: ☐ Desktop ☐ Laptop ☐ Other (please specify):_____

Type: ☐ PC ☐ UNIX Workstation ☐ Other (please specify):_____

PC Processor: ☐ 386 ☐ 486 ☐ Pentium ☐ Other (please specify):_____

COM port: ☐ COM1 25 pin ☐ COM2 9 pin ☐ Other (please specify):_____

Cable: ☐ Straight-thru DB25 (all 25 pins) ☐ EIA/TIA-232 DB25 to DB9 (factory-made)
☐ EIA/TIA-232 DB25 (pins 1-8, 20, 22 only) ☐ Straight-thru DB25 with DB25 to DB9 converter
☐ Straight-thru DB25 to DB9 (factory-made) ☐ EIA/TIA-232 DB25 with DB25 to DB9 converter

Operating System (OS) SW: ☐ MS Windows 3.1 ☐ Windows 3.11 ☐ WFW 3.11
☐ Windows 95 ☐ Windows 98
☐ UNIX (specify vendor and version):_____
☐ Other (please specify): _____

TCP/IP Software: ☐ No ☐ Yes (specify vendor and version): _____

Dialup PPP SW: ☐ No ☐ Yes (specify vendor and version): _____
☐ Manual Dial ☐ Remote Control ☐ Automated Dialing

Web Browser: ☐ No ☐ Yes (specify vendor and version): _____

POP3 email SW: ☐ No ☐ Yes (specify vendor and version): _____

Is your computer accredited to process SECRET Collateral information (level CS3)? ☐ Yes ☐ No

Do you have at least a SECRET Collateral clearance that is current? ☐ Yes ☐ No

For Your Information

Coming Events

Event	Location	Dates
AUSA/AAAA Aviation Symposium	Falls Church, VA	11-13 January 1999
1999 Tactical Wheeled Vehicle Conference	Monterey, CA	31 January – 2 February 1999
AUSA ARSOF Symposium and Exhibition	Pinehurst, NC	1-3 March 1999
IDEX '99, AUSA Pavilion	United Arab Emirates	14-18 March 1999
U.S. Army Ground Vehicle Survivability Symposium	Monterey, CA	29 March - 1 April 1999

The ARAT Community — Key Points of Contact

Agency	Name / e-mail	DSN Number	FAX Number
HQDA, DAMO-FDI	Mr. William M. McDowell mcdowwm@hqda.army.mil	227-4257	223-5336
HQ, TRADOC	Mr. Bob Miner minerr@monroe.army.mil	680-2664	680-3199
HQ, INSCOM	COL James P. Gibbons jpgibbo@vulcan.belvoir.army.mil	235-1791	656-1003
ARAT-PO	Mr. Joseph Ingrao ingrao@mail1.monmouth.army.mil	992-1337	992-5238
ARAT-TA	Mr. Norm Svarrer svarrer@eglin.af.mil	872-8899	872-8213 (C) 872-4268 (U)
ARAT-SE (CECOM)	Mr. Joseph Ingrao ingrao@mail1.monmouth.army.mil	992-1337	992-5238
ARAT-SC (FT. RUCKER)	Mr. George Hall hallg@rucker-emh3.army.mil	558-9334	558-1165
	CW4 Steve Woods stephen_woods@rucker-emh4.army.mil	558-1861	558-3468
AFIWC (KELLY AFB) (Army Flagging)	LTC Robert A. Wiedower rawiedo@afiwc.aia.af.mil	969-2021	(210) 977-2145
	Mr. Carl Brunner cbrunner@sdd.sri.com	969-2021	(210) 977-2145

The ARAT Bulletin Staff

Send comments, changes of address, and articles to:

U.S. Army CECOM
Software Engineering Center
ATTN: AMSEL-SE-WS-AI-EC
Fort Monmouth, NJ 07703-5207
FAX: 992-5238 (DSN); (732) 532-5238 (Commercial)

Editor-in-Chief
Mr. Joseph Ingrao, ARAT Project Office
Editor
Mr. Jody Brown, SRI International
Graphic Designer
Ms. Linda Axford, SRI International